La modernisation de la Convention 108 du Conseil de l'Europe

De Terwangne , Cécile

Published in:
Le développement du droit européen en matière de protection des données

Publication date:
2012

Document Version
le PDF de l'éditeur

La modernisation de la Convention 108 du Conseil de l'Europe

Cécile de Terwangne

Sommaire

A. Introduction

A l'approche des 30 ans de sa Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, le Conseil de l'Europe a entamé un travail de modernisation de ce texte afin de le mettre en phase avec les évolutions technologiques majeures apparues depuis sa naissance en 1981.

En effet, le paysage technologique a radicalement changé durant les trente années écoulées, ce qui a par ailleurs eu un impact considérable sur la société dans son ensemble, qui se verra qualifier de « société de l'information » et, plus récemment, de « société de surveillance ». C'est qu'Internet est passé par là, fabuleux réseau mondial avec bientôt le *Web 2.0* et l'interactivité mise au service de la diffusion des informations, du partage des données et de la communication universelle. *Google*, Wikipédia et les réseaux sociaux sont trois illustrations parmi tant d'autres des potentialités qu'offre désormais la technique en matière d'échange d'informations. Mais ils illustrent aussi les nouveaux défis suscités par ces potentialités au regard de la protection des données personnelles et de la vie privée. Ces défis n'ont cessé de se multiplier avec l'apparition des technologies de géolocalisation, de vidéosurveillance, le recours aux puces RFID, à l'Internet des Objets, aux identifiants biométriques, etc. L'opacité qui caractérise bon nombre de traitements de données effectués dans ce nouveau contexte n'est pas la moindre des sources d'inquiétude au regard de la protection des individus.

Le Comité conventionnel (T-PD) de la Convention 108 s'est dans un premier temps interrogé sur l'aptitude de la Convention à faire face à ces développements et à répondre adéquatement aux nouveaux défis apparus en offrant toujours dans ce nouvel environnement une protection correcte aux individus. Une étude a été réalisée pour identifier les éventuelles lacunes que présente la Convention 108 face aux nouvelles attentes ou nécessités de protection.[1] Cette étude à effectivement mis au jour une série de lacunes qui laissent l'individu démuni face à la nouvelle réalité qui l'entoure.

[1] *C. de Terwangne, J.-Ph. Moiny*, Les lacunes de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108) face aux développements technologiques, Rapport pour le Conseil de l'Europe, Strasbourg Novembre 2010, 60 p., disponible à l'adresse <http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports_and_studies_fr.asp>.

A la suite de cette étude, le Conseil de l'Europe a lancé une consultation publique en ligne entre janvier et mars 2011.[2] Cette consultation visait à permettre aux acteurs intéressés de par le monde, qu'ils proviennent du secteur public, du secteur privé, de la société civile ou des autorités de protection des données, de se prononcer sur l'avenir de la Convention. Les nombreuses réponses obtenues par le biais de cette consultation ont prouvé l'attention portée à la question de la révision de la Convention 108, révision couplée, il faut le dire, avec celle de la directive européenne 95/46 sur le même sujet ainsi qu'avec celle des Lignes directrices de l'OCDE de 1980 sur la protection de la vie privée et les flux transfrontières de données à caractère personnel.

Enrichi des apports résultant de la consultation publique, le travail de révision de la Convention a été mené par le Comité conventionnel T-PD au fil de nombreux mois. Il arrive presque à son terme à ce stade.[3]

Il convient encore de relever que les exercices de modernisation des deux textes européens « phares » en matière de protection des données, s'ils sont concomitants et peuvent être mis en parallèle, ne sont pas destinés à aboutir à un résultat parfaitement identique. Cela s'explique par le fait qu'il s'agit de deux instruments juridiques de nature différente, impliquant un niveau de rédaction des textes inégal, la directive européenne, et plus encore l'éventuel règlement européen qui lui fera suite, devant atteindre un niveau de précision des dispositions que ne doit certes pas présenter une convention internationale. Cela étant, il est impératif que les deux textes soient en totale cohérence sous peine de voir les Etats membres de l'Union européenne et signataires de la Convention 108 tiraillés entre des engagements contradictoires. Ce souci de parfaite cohérence a animé depuis le début les auteurs des travaux de révision de la Convention.

[2] <http://www.coe.int/t/dghl/standardsetting/dataprotection/Consultation_Modernisation_Convention_108_EN.pdf>. Voir *C. de Terwangne, J.-Ph. Moiny*, Rapport sur la consultation relative à la modernisation de la Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Conseil de l'Europe, Strasbourg juin 2011, disponible à <http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD-BUR_2011_10_fr.pdf>.

[3] Septembre 2012. Les travaux menés au Conseil de l'Europe sont très transparents. Les différents documents de travail témoignant de la progression des travaux de modernisation sont mis à disposition du public sur le site Internet de l'institution. Le dernier texte disponible est le Document final sur la modernisation de la Convention 108 (T-PD(2012)04rev) du 17 septembre 2012, <http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD_2012_04_rev_fr.pdf>.

Il faut savoir que la Convention a déjà été complétée le 8 novembre 2001 par un Protocole additionnel. Ce dernier a eu pour but de renforcer la mise en œuvre des principes contenus dans la Convention par l'ajout de deux nouvelles dispositions dont l'une traite des autorités de contrôle spécifiques à mettre en place par chaque Partie tandis que l'autre règle le sort des flux transfrontières de données à caractère personnel vers les pays non Parties à la Convention. Ces deux compléments n'apportent certes pas à eux seuls la réponse aux nouveaux défis qui se sont fait jour. Un travail de complète modernisation s'impose aujourd'hui.

B. Deux lignes d'action sages

Le travail de modernisation de la Convention 108 a été guidé par deux lignes d'action sages :

- la Convention a passé le cap des trente ans sans tomber dans l'obsolescence ; la révision doit avoir la même ambition et viser à légiférer pour une nouvelle période de trente ans. Cela signifie qu'il faut être attentif à garantir une neutralité technologique (I). Il ne faut pas concevoir le texte comme la réponse juridique à une technologie particulière qui risque sans aucun doute d'être dépassée dans un avenir plus ou moins proche.
- Les principes de protection contenus dans la Convention, qui présentent une grande similitude avec ceux contenus dans les Lignes directrices de l'OCDE et qui ont été qualifiés de « *Fair Information Principles* », se sont révélés pertinents pendant trente ans ; il convient de ne pas les abandonner (II). C'est un exercice de mise en adéquation avec les nouveaux défis qui se sont fait jour du fait des développements techniques qu'il s'agit et non de faire table rase d'un passé qui serait considéré comme dépassé.

I. Neutralité technologique

La neutralité technologique n'est pas prise ici dans son acception courante. Habituellement, elle signifie qu'un texte législatif ne devrait pas faire de discrimination entre les diverses techniques susceptibles d'être utilisées ni privilégier l'utilisation d'une technologie ou d'un moyen de communication (technologie de l'information ou papier) au détriment d'un autre.[4] Le souci

[4] <http://fr.jurispedia.org/index.php/Accueil>; *Philippe Gautrais*, Guide relatif à la gestion des documents technologiques, Fondation du Barreau du Québec, 2005, 8, disponible à l'adresse <http://lccjti.ca/definition/neutralite-technologique/>.

de neutralité technologique est pris ici dans le sens du souci d'élaborer un texte normatif détaché d'un contexte technologique trop particulier. Il ne s'agit pas de légiférer en fonction d'un outil technologique spécifique ou de formuler des principes de protection en se focalisant sur l'existence d'une technologie. Au risque déjà mentionné de désuétude des principes dès que la technologie sera dépassée ou abandonnée s'ajoute le risque d'inadaptabilité des règles énoncées aux nouvelles technologies qui ne manqueront pas d'émerger.

Ainsi, la traçabilité des choses et des individus par le biais des puces RFID (*radio frequency identification*), par exemple, suscite des inquiétudes. La réflexion sur la nécessité d'instaurer dans la Convention révisée un « droit à ne pas être tracé » a été soumise à la consultation publique évoquée *supra*. Il en est ressorti que l'instauration d'un tel droit dans la Convention ne serait pas opportune car elle viendrait clairement en réponse à un outil technique ciblé, les puces RFID. Il a été jugé préférable de traiter de cette question spécifique dans un instrument juridique sectoriel séparé, plus détaillé (une recommandation).

Le concept de « fichier automatisé »[5] présent dans la version de 1981 de la Convention 108 a en fait une connotation technologique datée qui pourrait compromettre la neutralité du texte de même que sa large application étant donné que cette notion n'a plus la même pertinence dans la réalité d'Internet et du *cloud computing*. Il a été décidé d'abandonner cette terminologie au profit de celle utilisée par la directive européenne 95/46 depuis 1995. C'est donc la notion de « traitement de données » qui est adoptée. Aux termes de l'article 2, c), du projet de texte révisé, on entend par là

> « toute opération ou ensemble d'opérations effectuées sur des données à caractère personnel, notamment la collecte, l'enregistrement, la conservation, la modification, l'extraction, la communication, la mise à disposition, l'effacement, la destruction des données, ou l'application d'opérations logiques et / ou arithmétiques aux données ;
>
> lorsque aucun procédé automatisé n'est utilisé, le traitement de données s'entend des opérations effectuées au sein d'un ensemble structuré établi selon tout critère qui permet de rechercher des données à caractère personnel ».

En conséquence logique, *l'expression « maître du fichier »* (« *controller of the file* » dans la version anglaise) est supprimée pour faire place à celle de « responsable du traitement » (« *controller* »). Cette expression signifie aux termes du projet de texte :

[5] Art. 2, b), de la Convention : « 'fichier automatisé' signifie : tout ensemble d'informations faisant l'objet d'un traitement automatisé ».

« la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, dispose du pouvoir de décision à l'égard du traitement de données ».[6]

Alors que cet acteur principal dans le traitement de données à caractère personnel était identifié dans la version initiale de la Convention comme étant la personne compétente pour décider de la finalité du fichier automatisé, des catégories de données visées et des opérations qui leur seront appliquées, il est cette fois recouru à un critère moins détaillé mais destiné à éclairer davantage sur le rôle décisif du responsable du traitement à l'égard du traitement effectué sur les données. C'est donc la personne qui exerce le pouvoir de décision sur ce traitement. Ce pouvoir de décision peut porter sur les finalités, les conditions, les moyens utilisés pour traiter les données, ainsi que sur les motifs justifiant le traitement, voire le choix des données à traiter. Une autre nouveauté réside dans le fait que le rôle de responsable du traitement pourra être dorénavant tenu par plusieurs personnes conjointement.

II. Maintien des *Fair Information Principles* avec les ajustements nécessaires

Ainsi qu'on l'a dit, une série de principes de protection présents dans la Convention de 1981 ont fait leurs preuves et ont remarquablement résisté à l'outrage du temps. Ils se sont révélés adéquats et efficaces dans des contextes technologiques et sociétaux qui n'ont pourtant cessé d'évoluer durant les trente années écoulées. C'est principalement leur rédaction sous forme de principes généraux qui leur a donné cette qualité d'adaptabilité et cette aptitude à être transposés dans des contextes radicalement différents.

Il convient de conserver ces principes de protection. Pour certains d'entre eux, on verra qu'il s'avère quand même nécessaire d'y apporter certains ajustements dans le but de les renforcer, les affiner ou les compléter.

1. Principe de loyauté

Au titre des principes à maintenir figure tout d'abord l'exigence de loyauté de la collecte.[7] Toutefois, cette loyauté ne devrait plus être limitée à la collecte mais valoir pour l'ensemble des opérations effectuées lors du traitement des données. La formulation de cette exigence élargie devient en conséquence :

[6] Article 2, d), du projet de texte.

[7] Exigence inscrite à l'art. 5, a), de la Convention.

« Les données à caractère personnel faisant l'objet d'un traitement sont traitées loyalement et licitement ».[8]

La loyauté induit que l'ensemble des opérations effectuées sur les données soient réalisées dans la transparence pour les personnes concernées, et sans tromperie. Le principe de loyauté est donc lié au devoir de transparence. On verra par la suite qu'une formulation plus explicite du devoir de transparence fait partie des modifications envisagées du texte de la Convention.

2. Principe de finalité

Pierre angulaire de la protection, le principe de finalité doit impérativement être conservé. Aux termes de ce principe ayant subi quelques ajustements rédactionnels, les données à caractère personnel doivent être « collectées pour des finalités explicites, déterminées et légitimes et ne pas être traitées de manière incompatible avec ces finalités ».[9]

Ce principe est fondamental dans la protection des données. En exigeant que les responsables de traitement déterminent dès le départ le but précis de leur démarche, on fournit le fil rouge qui permettra de savoir quelles données peuvent être collectées et utilisées pour servir ce but, quelles actions peuvent être réalisées avec ces données, à qui elles pourront être communiquées et combien de temps elles pourront être conservées. Seules les opérations et les communications compatibles avec les finalités de départ sont admises.

Tout part de la détermination d'une ou de plusieurs finalité(s) de base. Précision supplémentaire apportée au texte initial, il est demandé que la finalité soit explicite. Cette caractéristique vient appuyer le souci de transparence renforcée né pour contrecarrer l'opacité qui règne aujourd'hui dans les traitements de données.

3. Qualité des données

Les exigences liées à la qualité des données se sont révélées indispensables et pertinemment formulées. Elles ont traversé le temps sans prendre une ride et sont toujours d'actualité. Elles ne doivent donc pas subir de modification. Il s'agit donc toujours bien d'exiger que les données soient « adéquates, per-

[8] Art. 5, § 3, a), du projet de texte.

[9] Art. 5, §3, b), du projet de texte. Le texte initial stipule que les données sont « enregistrées pour des finalités déterminées et légitimes et ne sont pas utilisées de manière incompatible avec ces finalités ».

tinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées » ainsi que « exactes et si nécessaire mises à jour ».[10]

Il semble toutefois opportun d'insérer un *principe de minimisation des données*. Il convient d'insister sur le fait que les responsables de traitement ne doivent collecter que le minimum nécessaire de données. C'est une invitation explicite à la modération. L'exigence de ne traiter que des données pertinentes par rapport à la finalité conduit déjà à réduire la quantité de données convoitées. Cela ne s'est toutefois pas avéré suffisant car les données pertinentes étant celles qui présentent un lien d'utilité au regard de la finalité, elles ont pu être définies largement dans la réalité. L'exigence de données non excessives, quant à elle, signifie que, même pertinentes, les données qui induisent une atteinte excessive à la personne concernée ne doivent pas être traitées. C'est le cas notamment de la communication à l'employeur d'un avis du médecin du travail qui révélerait en détail l'état de santé d'un travailleur. Quoique pertinentes pour permettre à l'employeur de vérifier l'aptitude au travail de la personne concernée, ces données médicales sont excessives. On ne doit admettre que la communication d'un constat d'aptitude ou d'inaptitude sans développements détaillés. Dans sa version actuelle, la Convention 108 oblige donc déjà à réduire la collecte de données à caractère personnel, ce qui peut être vu comme une facette du principe de minimisation des données. Mais celui-ci va plus loin en exigeant de limiter au minimum nécessaire les données traitées.

D'un côté pratique, cette exigence de minimisation peut être rencontrée par le recours à des techniques d'anonymisation ou de pseudonymisation. Mais on peut très efficacement honorer ce principe en recourant à des solutions à caractère relativement peu technologique. Ainsi, on peut exiger que les paramètres par défaut de diverses applications renforcent la protection de la vie privée au niveau des quantités de données personnelles traitées, plutôt que ne la fragilise. Cela peut conduire à ce que, par défaut, un navigateur limite au maximum les informations qui sont envoyées aux sites web dans le sillage des visites effectuées par un utilisateur, ou un réseau social ne rende pas les informations qu'il contient visibles du monde entier, par exemple.

On notera que l'ensemble des autorités nationales de protection des données des Etats membres de l'Union européenne ont demandé que cet aspect du principe de minimisation soit désormais consacré dans la législation,[11] de

[10] Art. 5, c) et d), de la Convention.

[11] Groupe de l'article 29, Avis 2/2008 sur la révision de la directive 2002/58 concernant la protection de la vie privée dans le secteur des communications électroniques, WP 150, 15 mai 2008 ; Article 29 Working Party and Working Party on Police and Justice, WP 168, The Future of Privacy – Joint contribution to the Consultation of the European

même que le Contrôleur européen à la Protection des Données.[12] La Commission européenne a pour sa part adopté des actions pour promouvoir les technologies renforçant la vie privée (PETs) qui permettent de réduire le traitement de données à caractère personnel.[13] La résolution de Madrid a, quant à elle, rattaché au principe de proportionnalité l'exigence de limiter au minimum nécessaire les données faisant l'objet d'un traitement.[14]

En conséquence, l'exigence de qualité des données devrait prendre la forme suivante :

> « les données à caractère personnel faisant l'objet d'un traitement sont adéquates, pertinentes, non excessives et limitées au minimum nécessaire par rapport aux finalités pour lesquelles elles sont traitées. »[15]

4. *Droits des personnes concernées*

Si des droits sont déjà reconnus aux sujets de données depuis 1981, tels le droit d'accès aux données, le droit de rectification de celles-ci et le droit de recours, ces droits se voient renforcer par l'exercice de modernisation du texte. D'autres droits devraient en outre compléter la liste des garanties offertes aux personnes concernées.

Les développements relatifs à l'ensemble des droits, tant anciens que nouveaux, sont réservés au point H *infra*.

C. Liens entre la protection des données et d'autres valeurs

Le Comité conventionnel T-PD a souhaité que soit mis correctement en exergue le lien existant entre la protection des données et d'autres valeurs.

Ce lien n'était pas absent de la première version de la Convention puisqu'il était spécifié que l'objet du texte consistait à garantir aux individus

Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data, adopted on 1 December 2009, §53.

[12] EDPS Opinion on Promoting Trust in the Information Society by Fostering Data Protection and Privacy, 18 March 2010. Notamment: "the EDPS recommends the Commission to [...] propose to include a general provision on Privacy by Design in the legal framework for data protection." (point 38).

[13] Communication de la Commission européenne sur les technologies renforçant la protection de la vie privée, 2 mai 2007, COM(2007)228 final.

[14] Madrid Resolution, Article 8, § 2 : « In particular, the responsible person should make reasonable efforts to limit the processed personal data to the minimum necessary. »

[15] Art. 5, § 3, c), du projet de texte.

la protection de l'ensemble de leurs droits, parmi lesquels le droit à la vie privée, à l'égard du traitement des données à caractère personnel les concernant, ce qui correspondait à la « protection des données » était-il précisé entre parenthèses. Il s'agit cette fois de stipuler que le but de la Convention est de garantir à toute personne physique

« la protection des données à caractère personnel, contribuant au respect de *ses droits et libertés fondamentales, et notamment de son droit à la vie privée*, à l'égard du traitement de ses données à caractère personnel ».[16]

D'autres droits et libertés que la seule vie privée entrent en effet en ligne de compte, telle la liberté de se déplacer, celle de se loger, celle de trouver un emploi, celle de s'informer et de s'exprimer en toute transparence, etc.[17] « Ainsi, pour parler de la liberté d'expression et de la liberté d'association, comment imaginer que celles-ci puissent survivre si la personne se sait surveillée dans ses communications et ne peut à certains moments s'exprimer anonymement si la technologie garde systématiquement trace de ses messages ? La liberté de s'informer suppose que l'information ne soit pas filtrée, que l'on ne soit pas conduit, profilage aidant, à son insu ou malgré soi, vers l'information qu'autrui souhaite nous voir consommer. Pire, la même technique de profilage peut amener l'auteur du profilage à priver de certains services ou informations un consommateur pour lequel il estime qu'il est peu rentable de l'autoriser à y avoir accès. »[18]

Il a aussi semblé important de clarifier le Préambule sur ce point. Il est ainsi fait mention dans le Préambule qu'il est désormais nécessaire de garantir la protection des droits et libertés de chacun, « notamment au moyen du droit de contrôler ses propres données et les usages qui sont faits de telles données ». On notera que ce qui est évoqué, c'est un droit de contrôle reconnu à l'individu. La protection des données est en effet une émanation du droit au respect de la vie privée pris dans la dimension d'autonomie personnelle[19] ou même de droit à l'autodétermination[20] qui y est liée, davantage

[16] Art. 1er du projet de texte.

[17] Voy. sur ce point les développements dans *C. de Terwangne, J.-Ph. Moiny*, Les lacunes de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108) face aux développements technologiques, *op. cit.*, p. 4-5.

[18] *Y. Poullet, J.-M. Dinant, C. de Terwangne et M.-V. Perez-Asinari*, L'autodétermination informationnelle à l'ère de l'Internet, Rapport pour le Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD), Conseil de l'Europe, Strasbourg, 18 novembre 2004.

[19] Pour la mise au jour de la dimension d'autonomie personnelle attachée au droit au respect de vie privée consacré à l'article 8 de la Convention européenne des droits de l'Homme, voy. Cour eur. D.H., *Pretty c. Royaume-Uni*, arrêt du 29 avril 2002, req. n° 2346/02 ; *Van Kück c. Allemagne*, arrêt du 12 juin 2003, req. n° 35968/97 ; *K.A. et A.D. c. Belgique*, arrêt du 17 février 2005, req. n° 42758/98 et 45558/99.

que dans le sens d'exigence de confidentialité attaché traditionnellement à la notion de vie privée. La protection des données c'est le droit à l' « autodétermination informationnelle ».[21] C'est en ce sens que l'Assemblée parlementaire du Conseil de l'Europe a veillé à compléter sa Résolution 428 (1970). Le droit au respect de la vie privée garanti par l'article 8 de la Convention européenne des Droits de l'Homme avait été défini par l'Assemblée en janvier 1970 dans la déclaration sur les moyens de communication de masse et les droits de l'Homme contenue dans cette Résolution comme « le droit de mener sa vie comme on l'entend avec un minimum d'ingérence ». Près de trente ans après l'adoption initiale de ce texte, l'Assemblée a précisé que « Pour tenir compte de l'apparition des nouvelles technologies de la communication permettant de stocker et d'utiliser des données personnelles, il convient d'ajouter à cette définition *le droit de contrôler ses propres données* ».[22]

La Charte des droits fondamentaux de l'Union européenne, devenue juridiquement contraignante depuis l'entrée en vigueur du Traité de Lisbonne, a pris l'option de distinguer explicitement les concepts de vie privée (article 7) et de protection des données (article 8).[23]

[20] Pour la reconnaissance explicite d'un droit à l'autodétermination ou l'autonomie personnelle contenu dans le droit au respect de la vie privée de l'article 8 CEDH, voy. Cour eur. D.H., *Evans c. Royaume-Uni*, arrêt du 7 mars 2006, req. n° 6339/05 (confirmé par la Grande Chambre dans son arrêt du 10 avril 2007) ; *Tysiac c. Pologne*, arrêt du 20 mars 2007, req. n° 5410/03 ; *Daroczy c. Hongrie*, arrêt du 1er juillet 2008, req. n° 44378/05.

[21] Voy. *Herbert Burkert*, Le jugement du tribunal constitutionnel fédéral allemand sur le recensement démographique, Droit de l'Informatique et des Télécoms 1985, 8-16 ; *Cécile de Terwangne*, Le rapport de la vie privée à l'information, in Droit des technologies de l'information. Regards prospectifs (sous la direction d'*E. Montero*), coll. Cahiers du CRID, n° 16, Bruxelles, Bruylant, 1999, p. 144 ; *Thierry Leonard* et *Yves Poullet*, Les libertés comme fondement de la protection des données nominatives, in *F. Rigaux*, La vie privée : une liberté parmi les autres ?, Travaux de la faculté de Droit de Namur, n° 17, Bruxelles, Larcier, 1992, pp. 231 et s ; *Yves Poullet, Antoinette Rouvroy*, Le droit à l'autodétermination informationnelle et la valeur du développement personnel: une réévaluation de l'importance du droit à la protection de la vie privée pour la démocratie, in *Karim Benyekhlef, Pierre Trudel*, Etat de droit et virtualité, Montréal 2009, pp. 157-222.

[22] Résolution 1165(1998) de l'Assemblée parlementaire du Conseil de l'Europe sur le droit au respect de la vie privée, adoptée le 26.06.1998 (c'est nous qui soulignons).

[23] Article 7 : « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications »
Article 8 : « 1. Toute personne a droit à la protection des données à caractère personnel la concernant ; »

L'évocation du contrôle ou de la maîtrise informationnelle au nom de l'autodétermination permet de démontrer clairement que la Convention n'est pas qu'un instrument défensif, visant à garantir la confidentialité des données ou à interdire le traitement de certaines données sensibles, mais qu'elle traduit une approche plus positive en ce qu'elle est la manifestation du droit à l'autodétermination informationnelle.

Face à la diversification et à l'intensification des traitements ainsi que des échanges de données, il est aussi apparu impératif de proclamer l'importance attachée à la *dignité humaine*. L'invocation de la dignité humaine entend rappeler que l'être humain est un sujet et ne peut être ramené à un simple objet de la surveillance et du contrôle d'autrui. C'est l'idée que l'Homme ne peut être soumis à la machine mais que celle-ci, au contraire, doit être à son service et qu'elle ne peut porter atteinte aux valeurs essentielles des individus.

Autonomie et dignité doivent permettre de rééquilibrer le rapport Homme-machine. L'intention n'est bien évidemment pas d'enrayer le progrès mais bien de l'accompagner et l'encadrer en évitant l'enthousiasme béat qui conduirait à avaliser toute nouveauté technique sans s'interroger sur la place qui est laissée à l'individu dans le nouvel environnement.

D. Définitions

I. Notion de donnée à caractère personnel

Il a été décidé de ne pas modifier la définition donnée en 1981 à la notion phare qu'est celle de donnée à caractère personnel. Après trente ans d'utilisation, cette notion est devenue familière et il serait malvenu de modifier une pièce si importante de l'édifice de protection. Elle couvre donc

« toute information concernant une personne physique identifiée ou identifiable ('personne concernée') ».

Toutefois, l'explication de la définition qui était apportée dans le Rapport explicatif de la Convention devrait être revue de façon à éclairer la portée de la définition d'un jour nouveau. Ainsi, le texte en projet prévoit de spécifier

« 2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. »

« 3. Le respect de ces règles est soumis au contrôle d'une autorité de protection des données. ».

qu'une personne physique ne sera pas considérée comme « identifiable » si cette identification nécessite des délais ou des activités déraisonnables pour le responsable du traitement ou pour toute personne auprès de qui le responsable du traitement pourrait raisonnablement obtenir l'identification. En outre, par « identifiable » on n'entend pas seulement référer aux éléments de l'identité civile d'un individu mais aussi à ce qui permet d'individualiser une personne parmi d'autres. L'individualisation devrait en conséquence pouvoir se faire par rapport à la personne concernée elle-même, mais également par rapport à un terminal (ordinateur, téléphone portable, etc.).[24]

II. Notion de traitement de données

L'abandon de la notion de « fichier automatisé » utilisée dans la version actuelle de la Convention, pour lui préférer celle de « traitement de données » se justifie au nom d'un souci de neutralité technologique et de capacité à traverser le temps. Il a dès lors été déjà évoqué sous le point dédié à la neutralité technologique *supra* (cf. point B.I.).

III. Notion de responsable de traitement

Il y a lieu de renvoyer à ce qui a été dit précédemment à ce propos (cf. point B.I.).

IV. Nouvelles notions

Deux notions font leur apparition dans la nouvelle mouture de la Convention : celle de *destinataire* et celle de *sous-traitant*.

La première est essentiellement liée à la question des flux transfrontières de données. Elle vise

« la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données ou à qui des données sont rendues accessibles ».[25]

[24] Voy. dans le même sens l'intéressante position prise par la Federal Trade Commission des Etats-Unis dans son document à destination du monde des affaires et des décideurs politiques : « Protecting Consumer Privacy in an Era of Rapid Change », Document FTC March 2012.

[25] Art. 2, e), du texte en projet.

L'adoption de la notion de sous-traitant répond, quant à elle, à la nécessité de désigner des acteurs qui jouent un rôle aujourd'hui déterminant dans les traitements de données. Le nouveau texte entend par là

« la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ».

Il s'agit donc de la personne, au sens large, qui travaille sous les instructions du responsable de traitement pour effectuer les tâches (généralement techniques) que ce dernier n'est pas à même d'effectuer et qu'il lui délègue. Le sous-traitant est une personne extérieure au responsable du traitement.

Cette catégorie d'acteurs joue un rôle prépondérant dans le contexte du *cloud computing*, notamment. Il a semblé indispensable aux membres du T-PD d'intégrer les sous-traitants dans le texte de la Convention afin d'encadrer quelque peu leur intervention dans les traitements de données et de leur voir confier une certaine responsabilité.[26] Et cela, même si la pratique a mis au jour les difficultés d'application que la notion soulevait. Il n'est en effet pas toujours évident de distinguer les notions de responsable du traitement et de sous-traitant. C'est particulièrement vrai lorsqu'on se trouve en présence d'une organisation complexe comme une entreprise multinationale ou un groupement d'entreprises.

E. Champ d'application

I. Critère de la juridiction

Il a été décidé au cours des travaux de révision de la Convention de faire désormais référence à la notion de « juridiction » plutôt qu'à celle de « territoire » pour définir le champ d'application de la Convention. Ainsi, alors que selon le texte de 1981, « Le but de la présente Convention est de *garantir, sur le territoire de chaque Partie, à toute personne physique*, [...] », l'article 1er énonce dans sa nouvelle version :

« Le but de la présente Convention est de *garantir à toute personne physique relevant de la juridiction des Parties*, quelles que soient sa nationalité ou sa résidence, la protection des données à caractère personnel, contribuant au respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement de ses données à caractère personnel ».

Cette modification vise à mettre le champ d'application spatial de la Convention 108 en phase avec celui de la Convention européenne des droits de

[26] Voy. ce qui est dit ci-dessous à propos des obligations prévues à l'article 8*bis* du projet de texte.

l'Homme qui dispose en son article 1er que « Les Hautes Parties contractantes reconnaissent à toute personne relevant de leur juridiction les droits et libertés définis au titre I de la présente Convention ». La proximité entre la Convention 108 et l'article 8 CEDH attestée par la Cour européenne des droits de l'Homme à maintes reprises plaide en faveur d'une mise en cohérence des champs spatiaux des deux textes.

Préférer le critère de juridiction à celui de territoire devrait aussi offrir une meilleure capacité d'adaptation du texte à une réalité mouvante qui fait de plus en plus fi d'un ancrage territorial.

II. Limite du champ d'application

Il a été relevé comme une lacune le fait que la Convention 108 ne présente pas une restriction à son champ d'application qu'on retrouve dans la grande majorité des textes de protection des données existant à ce jour. Il s'agit de *l'exclusion des traitements de données effectués « par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques »*.[27]

En réponse à cette lacune, il est proposé d'introduire une exception générale concernant les traitements de données à caractère personnel à but personnel. La justification réside dans ce qu'on ne peut au nom de la protection

[27] Selon la formule de l'art. 3.2 de la directive 95/46. Cette exception est reprise dans toutes les législations des Etats membres de l'Union européenne (à l'invitation de la directive 95/46). L'APEC Privacy Framework a introduit une restriction du même type à son champ d'application par le biais d'une exception apportée à la définition de *personal information controller*. Ainsi, est exclu de cette définition tout individu « who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs » (APEC Privacy Framework, November 2004, disponible à l'adresse <http://www.apec.org/content/apec/apec_groups/som_special_task_groups/electronic_commerce.html>, Part II Scope, § 10). Le commentaire de cette disposition apporte cet éclaircissement : « Individuals will often collect, hold and use personal information for personal, family or household purposes. For example, they often keep address books and phone lists or prepare family newsletters. The Framework is not intended to apply to such personal, family or household activities ». La Résolution de Madrid, texte, issu d'un travail conjoint des autorités de protection des données de cinquante pays sous la houlette de l'Agence espagnole de la protection des données, admet, elle, que les lois nationales prévoient une exclusion du champ d'application pour les traitements réalisés par une personne physique dans le cadre d'activités exclusivement en lien avec sa vie privée (« private life ») et familiale (Article 3, § 2) (Madrid Resolution : Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data, disponible à l'adresse <http://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_es.pdf>).

des données d'autrui violer l'intimité de celui qui traite des données dans le cadre de sa vie privée et familiale.

La portée de cette exception doit cependant tenir compte de changements majeurs apportés par Internet dans la délimitation des sphères publique et privée. La pertinence et la portée d'une telle exception ont pris ainsi une grande importance avec le développement du *Web 2.0* et l'utilisation exponentielle de ses blogs, ses réseaux sociaux et son Twitter, par des particuliers qui fournissent désormais eux-mêmes des contenus dans lesquels figurent souvent des données à caractère personnel sous forme d'informations, de photos ou de vidéos. Recourir à ces médias est un moyen courant aujourd'hui pour s'exprimer, faire part de ses activités et de ses relations avec des tiers. C'est à la fois Internet comme lieu et moyen d'expression pour les individus en tant que citoyens et ce qu'on a appelé « *le Web 2.0 pour les loisirs* ».[28] Cet « Internet des loisirs » illustre parfaitement ce mélange de finalités personnelles et familiales et de l'utilisation d'un mode public d'expression qui vient contredire la vocation « privée » des données partagées.

Cette réalité a pour conséquence qu'il n'est pas évident d'accepter ou de refuser purement et simplement l'application d'une exception telle celle qui est envisagée ici, dans le nouvel environnement technologique. "The overall problem is that the granting of a full exemption from data protection requirements to anyone who uploads materials to the Internet as a private individual would lead to easy circumvention of the rules and, in an age of user-generated content, would fundamentally undermine data protection (and privacy) itself; yet the full imposition of the law to all such individuals would seem excessive and, because of the sheer numbers, would be largely unenforceable. The question – the challenge – is then perhaps whether a middle way may be found ?"[29]

Devant le défi de trouver un équilibre entre ne pas empiéter sur les activités personnelles des individus et néanmoins offrir une protection à autrui quand ces activités personnelles s'appuient sur des outils du *Net*, il est proposé d'introduire l'exception envisagée mais de la restreindre explicitement à la sphère personnelle. Ce qui signifie que la Convention devrait s'appliquer pleinement dès que des données à caractère personnel sont accessibles à

[28] Discours « L'Internet du futur: l'Europe doit jouer un rôle majeur » de *Mme Reding*, Commissaire européenne DG Société de l'Information et des Médias, à propos de l'Initiative «Futur de l'Internet» du Conseil Européen de Lisbonne (2 février 2009).

[29] *D. Korff*, Data protection laws in the EU: The difficulties in meeting the challenges posed by global social and technical developments, EC Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments, WP 2, 20 January 2010, p. 8.

des personnes externes à la sphère personnelle ou domestique. Cela conduit à la formulation suivante :

« La présente Convention ne s'applique pas aux traitements de données effectués par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques à moins que les données ne soient intentionnellement rendues accessibles à des personnes ne relevant pas de la sphère personnelle ».[30]

La sphère personnelle peut être définie en faisant intervenir différents critères. Parmi ces critères on trouve celui retenu par la Cour de Justice de l'Union européenne dans son arrêt *Lindqvist*[31] et repris par la Cour à plusieurs reprises par la suite. La CJUE a commencé par dire que l'exception doit être interprétée comme « visant uniquement les activités qui s'insèrent dans le cadre de la vie privée ou familiale des particuliers ».[32] Elle a ensuite fait remarquer que ce « n'est manifestement pas le cas du traitement de données à caractère personnel consistant dans leur publication sur Internet de sorte que ces données sont rendues accessibles à un nombre indéfini de personnes ».[33] Le critère retenu est donc le fait de rendre les données accessibles à un nombre indéterminé de personnes. Si ce critère est assurément éclairant pour déterminer si l'on sort de la sphère privée d'un individu, on ne peut l'inverser et estimer que rendre accessibles les données à un nombre défini de personnes permet de demeurer dans la sphère privée. Ce qui se passe sur les réseaux sociaux où l'on partage les informations avec un nombre certes défini mais parfois très élevé de personnes montre les limites du critère du nombre de destinataires. C'est la qualité du cercle des destinataires qui compte, leur nombre pouvant servir d'indice pour établir cette qualité. Un nombre même défini mais trop élevé fera inévitablement douter de la qualité personnelle du lien unissant celui qui traite les données à ceux avec qui il les partage.

F. Principes de protection

On a déjà évoqué plus haut les principes de base de la protection des données qui sont maintenus moyennant le cas échéant quelques aménagements rédactionnels ou de fond. Il s'agit à présent de présenter deux éléments qui ont été introduits dans ces principes de base, centrés sur la légitimité des traitements de données.

[30] Art. 3, 1*bis* du projet de texte.

[31] C.J.C.E., 6 novembre 2003 (*Lindqvist*), C-101-01, *Rec.* p. I-12971, par. 43 et 44.

[32] C.J.C.E., arrêt *Lindqvist*, par. 47.

[33] *Ibidem*.

I. Principe de proportionnalité

Dans sa version actuelle, la Convention 108 ne contient pas de formulation explicite du principe de proportionnalité. Selon ce principe, l'atteinte aux intérêts de la personne concernée ou à des intérêts collectifs qu'induit le traitement des données ne peut être disproportionnée par rapport à l'intérêt que le traitement des données représente pour son responsable. Seule la proportionnalité des données collectées et traitées est évoquée par la Convention[34] mais non celle du traitement dans son ensemble.

La jurisprudence de la Cour européenne des droits de l'Homme exige un juste équilibre entre les intérêts publics et privés en jeu lors de la mise en œuvre de traitements de données. Dans son arrêt *S. et Marper*,[35] la Cour a ainsi affirmé que le traitement de données doit être proportionné, c'est-à-dire approprié par rapport aux buts légitimes poursuivis, nécessaire dans la mesure où il n'existe pas d'autres mesures appropriées moins attentatoires aux intérêts, droits et libertés des personnes concernées ou de la société, et qu'il ne peut induire une atteinte démesurée à ces intérêts, droits et libertés par rapport aux bénéfices attendus par le responsable du traitement.

Il est devenu crucial aujourd'hui d'inscrire cette obligation qui peut servir de rempart face aux risques de certains développements techniques (notamment les traitements insoupçonnés qui foisonnent sur Internet) et au recours très (abusivement ?) répandu au consentement des personnes concernées pour traiter leurs données. Si la présence d'un consentement permet de présumer la légitimité d'un traitement, la mise en balance des intérêts en présence et la vérification de l'équilibre atteint offre une sauvegarde bienvenue quand on songe aux défauts trop souvent attachés au consentement (information insuffisante de la personne concernée, manifestation du consentement déduite de la non-modification de conditions par défaut, etc.).

Il a donc semblé impératif d'intégrer une formulation expresse de la condition de proportionnalité des traitements de données. Il est ressorti en outre des discussions portant sur la modernisation qu'il serait important d'insister sur le fait que c'est à tout moment, depuis la conception d'un traitement jusqu'à sa mise en œuvre et son aboutissement, pour toutes les opérations envisagées, qu'il faut être vigilant quant au respect du principe de proportionnalité.

En conséquence, le projet de texte formule la règle de la sorte :

[34] Cf. *supra*, point B.II.3.

[35] Cour eur. D.H. (Gr. Ch.), *S. et Marper c. Royaume-Uni*, 4 décembre 2008, req. nos 30562/04 et 30566/04, § 118.

« Le traitement de données doit être proportionné à la finalité légitime poursuivie et refléter à chaque étape du traitement un juste équilibre entre tous les intérêts en présence, qu'ils soient publics ou privés, ainsi que les droits et les libertés en jeu ».[36]

II. Hypothèses de légitimité des traitements de données

Dans un souci d'éclairer les acteurs devant se plier aux principes de protection, il est proposé d'introduire une disposition qui, à l'instar de ce qui existe dans la directive 95/46, liste les hypothèses dans lesquelles les traitements de données à caractère personnel sont légitimes. Une telle disposition a d'ailleurs été réclamée par de nombreux acteurs ayant répondu à la consultation lancée par le Conseil de l'Europe, évoquée à l'entame de cette contribution. L'article 5 initial de la Convention ne mentionne rien de la sorte. La Convention ne réservait ainsi jusqu'ici aucune place au consentement de l'individu.

Il est désormais proposé d'exiger soit le *consentement* des personnes concernées, soit une *obligation légale* ou *contractuelle*, soit un *intérêt légitime prépondérant*, comme condition au traitement de données.[37] Il est clair qu'il ne conviendrait pas pour un traité international d'opter pour un libellé trop détaillé de la liste des hypothèses retenues. Il faut s'en tenir à des formulations générales invitant les Etats à dessiner de manière plus précise les contours des hypothèses énoncées.

Pour être valable, *le consentement* doit être à tout le moins spécifique, libre et éclairé. Cette dernière qualité va de pair avec une obligation d'information qui devrait peser sur le responsable du traitement, obligation qui n'existe pas encore à l'heure actuelle dans la Convention mais qui est prévue dans sa version modernisée (voy. *infra*, point I.I.). L'exigence d'un consentement explicite et non équivoque fait encore l'objet de discussion au sein du T-PD. Un consensus ne s'est pas encore dessiné pour aller aussi loin dans les exigences pesant sur le consentement, même s'il est clair qu'une telle exigence conduirait à garantir la qualité des consentements exprimés et apporterait dès lors une réponse aux critiques émises à propos des consente-

[36] Art. 5, § 1.

[37] Le nouvel article 5, § 2 dispose que
« Chaque Partie prévoit que le traitement de données ne peut être effectué que si :
a. la personne concernée a donné son consentement de manière [explicite, non-équivoque], spécifique, libre et éclairée, ou
b. ce traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie, ou
c. ce traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis, ou
d. ce traitement est prévu par le droit interne pour un intérêt légitime prépondérant. ».

ments recueillis.[38] La forme et les conditions du consentement sont en effet source de grande préoccupation : des situations telles que la non-opposition aux conditions d'utilisation des données proposées par le fournisseur de service sur une page internet « subalterne », le non « décochage » de cases précochées, la non-modification des paramètres par défaut, sont avancées comme correspondant à des consentements. L'opacité des réseaux, le fait que de nombreux traitements de données échappent aux personnes concernées et le fait que nombre d'individus ne prennent pas la juste mesure des implications que les traitements présentent, conduisent à s'inquiéter de ces consentements présupposés.

G. Données sensibles

I. Les deux approches

L'identification de catégories particulières de données auxquelles on réserve une protection plus élevée est liée aux risques accrus de porter préjudice aux individus sur la base du traitement de ces données. C'est principalement le risque de discriminations illégitimes ou arbitraires qui est lié à ces données. Les Principes directeurs de l'ONU pour la réglementation des fichiers informatisés contenant des données à caractère personnel[39] mettent d'ailleurs bien en évidence ce risque. Ils contiennent en effet une disposition consacrée aux données sensibles intitulée « Principe de non-discrimination ».[40] La résolution de Madrid indique elle aussi très clairement le lien entre le régime spécial accordé aux données sensibles et le risque de discrimination illégitime. Ce texte ajoute cependant le risque de telles données d'affecter la sphère la plus intime des sujets de données, ainsi que, tout simplement, le

[38] Article 29 Working Party and Working Party on Police and Justice, WP 168, The Future of Privacy – Joint contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data, adopted on 1 December 2009, §§ 65-68.

[39] Résolution 45/95 de l'Assemblée générale des Nations Unies du 14 décembre 1990.

[40] Article 5, Principe de non-discrimination : Sous réserve des cas de dérogations limitativement prévus sous le principe 6, les données pouvant engendrer une discrimination illégitime ou arbitraire, notamment les informations sur l'origine raciale ou ethnique, la couleur, la vie sexuelle, les opinions politiques, les convictions religieuses, philosophiques ou autres, ainsi que l'appartenance à une association ou un syndicat, ne devraient pas être collectées.

risque sérieux que ces données présentent, en cas d'abus, pour la personne concernée.[41]

La question des données sensibles suscite l'éternel débat entre tenants de l'hypothèse où c'est le contexte d'utilisation, la finalité du traitement envisagé qui rend les données sensibles et ceux qui estiment indispensable d'établir une liste de données sensibles par nature. Le recours à une telle liste déclenche automatiquement l'application d'un régime de protection renforcé lié au risque d'affecter la sphère la plus intime des individus ou d'engendrer des discriminations illégitimes ou arbitraires sur la base des données visées. Une telle liste permet donc d'évacuer toute interrogation contextuelle.

La solution retenue en 1981 a été celle de la liste préétablie mais n'est pas sans soulever un problème exposé ci-dessous. La solution proposée à présent est une combinaison entre les deux approches.

La définition des données sensibles présentée à l'article 6 de la Convention est effectivement extrêmement large du fait qu'elle qualifie comme telles les données « *révélant* l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, ... ».[42] Cela signifie que tombent dans cette catégorie, par exemple, les noms patronymiques qui révèlent indubitablement l'origine raciale, de même que toute photo d'une personne ; l'achat d'un ouvrage sur le Coran sur un site web peut quant à lui révéler les convictions religieuses, etc. Or, il est inconcevable de traiter systématiquement les noms, les photographies et certains achats comme des données sensibles bénéficiant d'un régime de protection particulièrement sévère. Ce ne sera que quand c'est justement l'élément sensible de la donnée qui est retenu par le responsable du traitement (sélection des personnes d'origine africaine ou japonaise, sur la base de leurs noms ; ou sélection des personnes de type tutsi, rom ou aborigène sur la base de leurs photos) que le régime protecteur, principalement justifié par le risque élevé de discrimination à partir des données traitées, se justifie.

D'une part, il est louable de retenir les données « révélant » des caractéristiques sensibles des personnes. Cela permet en effet de considérer comme sensibles des cas dans lesquels n'apparaît aucune donnée *a priori* sensible. Ainsi, les recherches sur *Google* de sites sur le pèlerinage de Saint Jacques de Compostelle pratiquées par un internaute, son achat de livres religieux, sa

[41] Avant de présenter une liste non exhaustive de données considérées comme sensibles, l'article 13, § 1, de la Résolution de Madrid indique « The following personal data shall be deemed to be sensitive : a. Data which affect the data subject's most intimate sphere ; or b. Data likely to give rise, in case of misuse, to : i Unlawful or arbitrary discrimination ; or ii A serious risk to the data subject ».

[42] C'est nous qui soulignons.

lecture d'une encyclique pontificale, etc. pourraient être traitées comme révélant une opinion religieuse.

D'autre part, retenir justement tout ce qui révèle une caractéristique sensible en arrive, ainsi qu'on l'a dit, à faire entrer dans cette catégorie de données énormément de données qui dans bien des cas ne sont pas traitées pour l'aspect sensible qu'elles véhiculent. Cela est excessif et risque d'ôter son sens à la notion de données sensibles au niveau de l'application concrète.

II. La proposition de modification

La solution trouvée tient donc dans la nouvelle formulation suivante proposée de l'article 6[43] rebaptisé « Traitement de données sensibles » :

« 1. Les traitements de données à caractère personnel pouvant présenter un risque grave pour les intérêts, droits et libertés fondamentales de la personne concernée, notamment un risque de discrimination, ne sont possibles qu'à la condition que le droit applicable prévoie des garanties appropriées de nature à prévenir ce risque venant compléter celles de la présente convention.

2. Présentent en particulier un tel risque :

a le traitement des données génétiques, des données relatives à la santé ou à la vie sexuelle et des données concernant des infractions, condamnations pénales et mesures de sûreté connexes,

b les données traitées pour l'origine raciale, les opinions politiques, l'appartenance syndicale, les convictions religieuses ou autres convictions qu'elles révèlent, et

c les données traitées pour l'information biométrique identifiante qu'elles contiennent. »

La différence majeure par rapport au texte de 1981 tient dans le fait que sans renoncer à l'élaboration d'une liste préétablie, il est proposé de tenir compte du contexte d'utilisation des données. Cette solution marie donc le principe d'une liste de données pointées comme sensibles mais ne déclenchant le régime de protection que si c'est l'élément sensible de la donnée qui est précisément recherché et traité (voy. l'article 6, §2, b) et c)). Certaines données par ailleurs suivent le modèle de 1981 : elles sont considérées comme sensibles en toutes circonstances et il suffit qu'elles fassent l'objet d'un traitement, quelle que soit la finalité de celui-ci, pour que le régime plus protecteur soit d'application (voy. l'article 6, §2, a)).

On remarquera que certaines catégories de données ont été ajoutées à la liste préexistante. Il s'agit premièrement des *données génétiques* considérées comme sensibles par nature en toute circonstance et donc rattachées à la liste

[43] A ce stade, les discussions au sein du T-PD portant sur la nouvelle formulation idéale de l'article sur les données sensibles sont encore intenses. La présentation qui suit correspond au texte fruit des discussions arrêtées fin septembre 2012.

de l'alinéa a). La Cour européenne des droits de l'Homme a exposé clairement dans son arrêt *S. et Marper* en quoi ces données soulevaient une préoccupation particulière au regard de la protection de la vie privée.[44] Elle a ainsi estimé que les profils ADN contiennent une quantité importante de données à caractère personnel uniques qui, même si objectives et irréfutables, permettent aux autorités d'aller bien au-delà d'une identification neutre (les profils ADN peuvent notamment être utilisés pour effectuer des recherches familiales en vue de découvrir les relations génétiques pouvant exister entre des individus). On peut ajouter que les données génétiques peuvent révéler des choses que l'individu ne souhaite peut-être pas lui-même connaître. Dans son analyse réalisée pour le Conseil de l'Europe en 1999, *Spiros Simitis* estimait déjà que « Aucune liste de données sensibles ne peut négliger les données génétiques sans que l'on s'interroge sur son sérieux. ».[45] Il signale ainsi : « Rien n'illustre mieux la nécessité de mettre à jour les listes que les données génétiques. [...] Aujourd'hui, il n'y a aucun doute qu'aucune autre catégorie de données ne donne d'informations aussi complètes sur les personnes concernées. Les risques du traitement de données à caractère personnel n'avaient donc jamais été aussi évidents auparavant. Qu'il s'agisse de la possibilité de trouver un emploi, des chances d'obtenir une assurance maladie ou des limites de la marchandisation croissante des individus, l'accessibilité des données génétiques détermine la réponse. »[46]

Deuxièmement, les données concernant les condamnations pénales, relevant elles aussi de l'alinéa a), se voient associer les *données concernant des infractions et celles concernant des mesures de sûreté connexes*.

Troisièmement, les *données révélant l'appartenance syndicale* font leur apparition dans la liste de l'alinéa b). Ces dernières données ne figuraient pas dans la liste de 1981 mais le Rapport explicatif de la Convention signalait que cette liste ne devait pas être considérée comme exhaustive et que les Etats Parties pouvaient ajouter d'autres catégories de données si le contexte sociologique l'imposait. L'exemple donné était précisément celui des informations sur l'appartenance syndicale. Il était relevé que dans certains pays ces informations sont considérées comme entraînant des risques pour la vie privée alors que dans d'autres pays elles ne sont considérées comme sen-

[44] Arrêt précité, §75.

[45] *Spiros Simitis*, Les données sensibles revisitées (1999), Examen des réponses au questionnaire du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE 108), Strasbourg, 24-26 novembre 1999.

[46] *Ibidem*.

sibles que dans la mesure où elles sont étroitement liées aux opinions politiques.[47]

Enfin, il convient de relever qu'une indication est apportée à propos des « *garanties appropriées* » que les Etats doivent prendre pour permettre que les données sensibles fassent l'objet de traitement. Ces garanties figurent déjà dans l'article 6 initial de la Convention mais rien ne vient les éclairer. L'interdiction pesant sur le traitement des données sensibles a pu donc jusqu'à présent être levée par des garanties jugées appropriées par les Etats parties sans aucune balise. Cette fois, deux éclaircissements sont apportés. Tout d'abord, il est indiqué que les garanties appropriées doivent venir en supplément des mesures de protection mises en place par la Convention. On ne peut donc se contenter de renvoyer à des mesures relevant du régime général pour rendre admissible le traitement de données sensibles. Ensuite, les garanties appropriées sont présentées comme celles de nature à prévenir le risque grave que le traitement des données sensibles fait peser sur les intérêts, droits et libertés fondamentales de la personne concernée, notamment le risque de discrimination.

H. Droits des personnes concernées

Certains droits sont déjà garantis à la personne concernée. L'exercice de modernisation de la Convention va déboucher sur le maintien de ces droits, le droit d'accès existant devant même être enrichi. Des droits nouveaux vont en outre faire leur apparition : droit d'opposition, droit de ne pas être soumis à une décision automatisée, droit de connaître le raisonnement qui sous-tend le traitement des données et droit à l'assistance d'une autorité de contrôle.

Il est à noter que l'article 8 dédié aux « Droits des personnes concernées »[48] ne contient aucune *limitation* aux droits qu'il énonce. Il ne faut pas en déduire que ces droits sont absolus et ne souffrent aucune restriction. Cela est dû à une particularité rédactionnelle de la Convention : plutôt que d'insérer dans chaque article les exceptions admissibles aux règles figurant à l'article en question, une disposition spécifique (l'article 9) est consacrée aux différentes exceptions envisageables pour la plupart des principes de protection contenus dans la Convention. Les restrictions sont laissées à la discrétion des Etats Parties qui peuvent prévoir celles qui leur paraissent nécessaires mais doivent respecter les conditions émises à l'article 9.

[47] Rapport explicatif, § 48.

[48] L'intitulé du texte de 1981 est « Garanties complémentaires pour la personne concernée ».

Enfin relevons encore avant de passer les divers droits en revue qu'il a été décidé lors des travaux de modernisation de ne pas proposer l'introduction explicite d'un « droit à l'oubli » dans le texte révisé de la Convention. Il a en effet été considéré que la conjugaison des garanties existantes peut offrir une protection efficace aux personnes concernées sans porter atteinte au droit à la liberté d'expression. Ainsi, la règle dérivant du principe de finalité, imposant une durée de conservation des données réduite en fonction de la finalité du traitement à atteindre conduit à l'effacement des données dès que celles-ci ne présentent plus d'utilité pour réaliser l'objectif du traitement. En outre, le droit de rectification et d'effacement des données incorrectes, incomplètes ou injustifiées, associé a un droit effectif d'opposition au traitement, apporte également une forme de réponse à la préoccupation liée au droit à l'oubli. Même si la réponse issue de cette combinaison de dispositions existantes ou à insérer dans la Convention n'est pas parfaitement satisfaisante sur le plan du droit à l'oubli, les auteurs de la modernisation de la Convention ont préféré s'en tenir à cela plutôt que de consacrer dans une Convention internationale un droit dont les contours sont mal déterminés et qui suscite encore aujourd'hui d'intenses débats car il se heurte de front avec la liberté d'expression et d'information, le devoir de mémoire et d'autres intérêts.

Les membres du T-PD envisagent de traiter de ce sujet par le biais d'une recommandation qui porterait sur les réseaux sociaux car il est vrai que c'est principalement dans ce contexte – même si pas exclusivement – que la question du droit à l'oubli numérique se pose aujourd'hui.

I. Droit de ne pas être soumis à une décision automatisée

Il a tout d'abord paru impératif pour les participants à l'exercice de modernisation de la Convention de consacrer en premier lieu le droit pour toute personne de

> « ne pas être soumise à une décision l'affectant de manière significative qui serait uniquement basée sur un traitement automatisé de données, sans que son point de vue soit pris en compte ».[49]

Présenté comme premier droit de la personne concernée, ce droit découle de la volonté farouche que l'Homme ne soit pas soumis entièrement à la machine. Il n'est pas souhaitable qu'une décision qui s'impose à un individu dépende des seules conclusions d'une machine.[50] C'est là l'expression de la prééminence à accorder à la dignité humaine.

[49] Art. 8, a), du projet de texte.

[50] Cf. *supra* ce qui est dit à propos de la dignité humaine.

Or, la technique est de plus en plus souvent utilisée aujourd'hui pour s'en remettre à un « ordinateur » et aux algorithmes qu'il applique pour décider du traitement à réserver à un individu (le considérer ou non comme fraudeur fiscal, ou comme cible de marketing, ou comme voyageur candidat terroriste, ...). Ainsi, « les nouvelles technologies entraînent dans leur sillage de nouvelles menaces : face à la multiplication des analyses de plus en plus automatisées de données toujours plus nombreuses et accessibles, les individus risquent d'être réduits à de simples objets, qui seront traités (ou qui pourront même faire l'objet de discrimination) sur la base de « profils » informatiques, de probabilités et de prévisions, sans possibilité de s'opposer aux algorithmes sous-jacents. À défaut de maintenir une protection des données très stricte, les décisions qui ont un « impact significatif » (par exemple, la décision de vous refuser un poste ou de ne pas même vous accorder un entretien d'embauche ; d'être arrêté à une frontière et éventuellement de se voir refuser l'entrée dans un pays ; d'être soumis à une surveillance intrusive, et éventuellement d'être arrêté, etc.) seront de plus en plus souvent motivées « par le fait que l'ordinateur a dit non » (même si les responsables ou le personnel prenant la décision ne peuvent la justifier complètement) ». [51]

II. Droit d'opposition

Il a été décidé d'inscrire le droit d'opposition au tableau des droits subjectifs destinés à permettre aux individus d'exercer une maitrise sur le sort réservé à leurs données, de leur permettre de mettre en œuvre leur autodétermination informationnelle. L'article 8 b, du texte en projet dispose en conséquence que

> « Toute personne doit pouvoir
> a. [...]
> b. s'opposer à tout moment pour des raisons légitimes à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement à moins que le traitement soit rendu obligatoire par la loi ou que le responsable du traitement puisse justifier de motifs légitimes prépondérants ».

Ce droit se justifie particulièrement lorsque le traitement des données ne repose pas sur le consentement des personnes concernées. Celles-ci, qui

[51] *LRDP Kantor Ltd, en association avec Centre for Public Reform*, Étude comparative sur les différentes approches des nouveaux défis en matière de protection de la vie privée, en particulier à la lumière des évolutions technologiques, Rapport final, Note de synthèse, disponible sur <http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_fr.pdf>, janvier 2010, p. 2.

n'ont pu exprimer leur point de vue à l'entame du traitement, retrouvent par le biais de ce droit la possibilité de faire valoir leurs arguments auprès du maitre du fichier pour le convaincre de renoncer à traiter leurs données. Ce droit est particulièrement important dans les hypothèses où le responsable a effectué lui-même, *a priori*, la mise en balance des intérêts en présence et a estimé que le résultat était équilibré et qu'il pouvait légitimement traiter les données. Grâce au droit d'opposition, la personne concernée retrouve l'occasion de contester le résultat de la mise en balance, à tout le moins dans son cas.

La formulation retenue à ce jour, très proche de celle figurant à l'article 19 de la proposition de règlement de l'Union européenne,[52] inverse opportunément la charge de la preuve concernant l'intérêt « prépondérant ». La personne concernée est juste tenue de faire valoir des « raisons légitimes » qui l'amènent à s'opposer au traitement de ses données. C'est au responsable de traitement qu'il incombe par contre d'avancer des motifs légitimes prépondérants et de prouver donc par là que son intérêt légitime prévaut sur les droits et intérêts de la personne concernée. Etant parfaitement éclairé sur le traitement qu'il effectue lui-même sur les données, il semble en meilleure position que la personne concernée pour argumenter sur la balance des intérêts en jeu.

Il est clair que dans le contexte technologique actuel où les traitements de données à l'insu ou sans recourir au consentement des personnes concernées se développent à foison, il est important de rééquilibrer la situation des intervenants en garantissant un droit aux personnes concernées de se manifester et de refuser les enregistrements et utilisations de leurs données quand elles viennent à en prendre connaissance. Il se peut aussi que les personnes avaient bien été informées des traitements envisagés mais n'ont pris la pleine mesure du sort réservé à leurs données, ou des implications que ces traitements pouvaient avoir sur d'autres intérêts, qu'après un certain temps. Dans de tels cas également, le droit d'opposition offre une solution opportune.

Il est à noter que le droit d'opposition ne doit pas être confondu avec le droit de rétractation du consentement. Pour les traitements de données reposant sur un consentement, il est possible pour la personne concernée de rétracter celui-ci.[53]

[52] Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (Règlement général sur la protection des données), COM (2012) 11/4, 25 janvier 2012.

[53] Moyennant le cas échéant le respect de conditions issues du droit national civil telle la condition de bonne foi.

III. Droit d'accès enrichi

Depuis plus de trente ans, les individus se voient garantir le droit d'avoir connaissance de l'existence de traitement de données à leur propos et de la teneur des informations faisant l'objet d'un traitement.

Il a été décidé d'enrichir ce droit d'accès et d'y intégrer le droit d'accéder sur demande à toutes les informations que le responsable est en principe tenu de communiquer spontanément aux personnes concernées.[54] Des exceptions pouvant exister à ce devoir de transparence spontanée, il se peut qu'un individu n'ait reçu aucune information particulière sur le traitement effectué avec ses données et souhaite connaître par exemple l'identité du responsable du traitement ainsi que ses coordonnées, ou les finalités du traitement, ou encore les destinataires des données. Il peut donc prendre l'initiative de réclamer ces informations.

Par ailleurs, le droit d'accès a aussi été enrichi pour couvrir l'accès à l'origine des données. Cette information est en effet cruciale car c'est souvent la source des données qui intrigue et interpelle les personnes concernées (comment ont-ils obtenu ces informations, qui les leur a communiquées ?). Par ailleurs, les renseignements sur l'origine des données permettent de vérifier la licéité de la communication ou de la collecte de celles-ci et éventuellement d'introduire un recours à l'encontre du premier détenteur des données (ce qui permet « d'arrêter l'hémorragie » si celui-ci diffuse illicitement les données en question). Enfin, en cas de problèmes liés à la qualité des données et de nécessité de correction, il devient possible de faire effectuer ces corrections à la source, ce qui évite la propagation ultérieure d'erreurs.

Dans la nouvelle formulation qui est proposée, le droit d'accès s'entend donc au droit pour chaque personne concernée d'

> « obtenir, à sa demande, à intervalle raisonnable et sans délai ou frais excessifs la confirmation de l'existence d'un traitement de données la concernant, la communication sous une forme intelligible des données traitées, toutes informations disponibles sur leur origine, ainsi que toute autre information que le responsable du traitement est tenu de fournir au titre de la transparence des traitements conformément à l'article 7*bis* paragraphe 1 ».[55]

[54] Voy. *infra* le point I.I.

[55] Art. 8, c), du projet de texte.

IV. Droit de connaître le raisonnement qui sous-tend le traitement des données

Dans le contexte technique actuel, il est un droit qui ne se trouve pas dans la Convention mais qui présente un grand intérêt, notamment face au déploiement exponentiel du phénomène de profilage. Il s'agit du droit d'avoir connaissance du raisonnement qui sous-tend le traitement de données dont les résultats lui sont appliqués.

Ce droit auquel on ne songeait pas en 1981 a fait son apparition par la suite.[56] Il a été proclamé dans la recommandation du Comité des Ministres du Conseil de l'Europe relative au profilage.[57] Il est tout d'abord relevé dans les considérants de ce texte : « Rappelant que toute personne doit avoir le droit d'accéder aux données la concernant et considérant qu'elle devrait connaître la logique qui sous-tend le profilage ; sachant que ce droit ne devrait pas porter atteinte aux droits et libertés d'autrui, en particulier ne pas nuire aux secrets commerciaux, à la propriété intellectuelle ou au droit d'auteur protégeant les logiciels, [...] ». Ensuite, la recommandation consacre le droit d'accès à cette information : « La personne concernée qui a fait, ou qui fait l'objet d'un profilage devrait pouvoir, à sa demande, obtenir du responsable du traitement, dans un délai raisonnable et sous une forme compréhensible, les informations suivantes : [...] b. la logique qui sous-tend le traitement des données à caractère personnel la concernant et qui a été utilisée pour lui attribuer un profil, au moins en cas de décision automatisée. »[58]

Dans la même ligne que ce qui a été reconnu en matière de profilage des individus, les auteurs de la révision de la Convention 108 ont estimé qu'il convenait de consacrer le droit à cette information particulière au sein même de la Convention. Il s'indique de dépasser les limites du profilage, même si un tel droit s'impose spécialement face au phénomène où l'on s'appuie sur

[56] La directive européenne 95/46 Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (J.O.C.E. n° L 281 du 23/11/1995, p. 31-50) consacre ce droit en son article 12 : « Les États membres garantissent à toute personne concernée le droit d'obtenir du responsable du traitement: a) [...] la connaissance de la logique qui sous-tend tout traitement automatisé des données la concernant, au moins dans le cas des décisions automatisées ».

[57] Recommandation du Comité des Ministres du Conseil de l'Europe CM/Rec(2010)13 sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, adoptée le 23 novembre 2010.

[58] Point 5. 1. b. de l'Annexe à la Recommandation CM/Rec (2010)13.

des « profils »[59] pour prendre des décisions au sujet d'une personne ou prévoir ses préférences, ses comportements et ses attitudes personnels.[60] Il est clair que même en dehors de l'hypothèse du profilage, on peut souhaiter comprendre ce qui se passe en accédant au raisonnement sous-tendant le traitement des données. Face au refus d'un crédit, aux résultats d'un examen, à la non-sélection d'une offre faite en réponse à un appel d'offres, etc., on peut légitimement souhaiter connaître les critères qui ont joué et le poids accordé à chacun d'eux pour évaluer la capacité de remboursement, corriger et évaluer l'examen ou apprécier la qualité de l'offre.

Ce droit risque d'ailleurs bien de devenir un des droits clés contribuant largement à la transparence et dès lors à l'auto-détermination informationnelle des individus car il permet à ceux-ci *non pas seulement de savoir* ce qui se passe avec leurs données, *mais bien de comprendre*. Il est donc proposé d'ajouter le droit suivant à la liste des garanties offertes à la personne concernée : le droit pour toute personne d'

« obtenir, à sa demande, connaissance du raisonnement qui sous-tend le traitement de données dont les résultats lui sont appliqués ».[61]

Il est à noter que ce droit pourra être limité par les Etats Parties dans le respect des conditions édictées à l'article 9 de la Convention pour toute restriction. Ce sera notamment le cas où cela est nécessaire dans une société démocratique pour protéger des « secrets protégés par la loi », comme par exemple des secrets commerciaux où découlant de la propriété intellectuelle.

V. Droit de rectification

Le droit de rectification a été accordé depuis l'origine aux personnes concernées. Il est maintenu moyennant les légères modifications de forme mises en relief dans l'énoncé qui suit. Toute personne se voit donc reconnaître le droit d'

[59] Le profil désigne « un ensemble de données qui caractérise une catégorie d'individus et qui est destiné à être appliqué à un individu » (point 1.d. de l'Annexe à la Recommandation CM/Rec (2010)13).

[60] Voy. la définition du « profilage » proposée par la Recommandation : « Le « profilage » est une technique de traitement automatisé des données qui consiste à appliquer un « profil » à une personne physique, notamment afin de prendre des décisions à son sujet ou d'analyser ou de prévoir ses préférences, comportements et attitudes personnels. ». (point 1.e. de l'Annexe à la Recommandation CM/Rec (2010)13).

[61] Art. 8, d), du projet de texte.

« obtenir *à sa demande*, le cas échéant, la rectification de ces données ou leur effacement lorsqu'elles ont été traitées en violation des dispositions du droit interne donnant effet *aux dispositions* de la présente Convention ».[62]

VI. Droit de recours

Un recours doit être mis à la disposition de toute personne qui voit ses droits bafoués, à qui par exemple le responsable du traitement n'a pas répondu ou les cas où celui-ci n'a pas corrigé ou effacé les données malgré une demande en ce sens ou n'a pas cessé le traitement des données alors que la personne concernée s'y était opposée. Ce droit existait déjà dans la version initiale de la Convention mais a été élargi pour être mis en adéquation avec l'augmentation des droits reconnus.

Cette disposition doit être lue en combinaison avec l'article 10 qui porte sur les « Sanctions et recours ». Il y est prévu que chaque Partie s'engage à établir des recours juridictionnels et non-juridictionnels appropriés visant les violations du droit interne donnant effet aux dispositions de la Convention. La nature des recours mis en place (civils, administratifs, pénaux) est laissée à la décision de chaque Etat Partie. On a pu constater que « La plupart des pays disposant d'une loi en matière de protection des données ont institué à cet égard une autorité de contrôle, généralement un commissaire, une commission, un ombudsman ou un inspecteur général. Ces autorités de contrôle dans le domaine de la protection des données fournissent un recours approprié lorsqu'elles sont dotées de compétences effectives et qu'elles jouissent d'une réelle indépendance dans l'exercice de leurs fonctions. Elles sont devenues partie intégrante du système de contrôle de la protection des données dans une société démocratique. »[63] Les autorités de contrôle doivent se voir confier des pouvoirs d'intervention,[64] mais ceux-ci peuvent se manifester en droit interne de différentes manières. A titre d'exemple, le Rapport explicatif du Protocole additionnel à la Convention précise : « l'autorité de contrôle pourrait avoir la possibilité d'obliger le maître du fichier à rectifier des données incorrectes ou collectées de manière illégale, de les effacer ou de les détruire, d'office ou si l'individu n'est pas en mesure d'obtenir les mêmes résultats en agissant lui-même. La possibilité pour l'autorité de contrôle de donner des injonctions au responsable du traitement qui n'est pas prêt à

[62] Art. 8, e), du projet de texte.

[63] Rapport explicatif du Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données, STE 181, du 8 novembre 2001, point 5.

[64] Art. 1er, § 2, a), du Protocole additionnel à la Convention.

communiquer les informations requises dans des délais raisonnables constituerait une transposition particulièrement efficace du pouvoir d'intervention ».[65]

VII. Droit à l'assistance d'une autorité de contrôle

Ainsi qu'on vient de le voir, les individus peuvent se tourner vers les autorités de contrôle nationales pour exercer leur droit de recours contre le non-respect d'un des droits qui leur sont garantis. Il faut pour cela que les autorités de contrôle disposent d'un pouvoir de trancher les litiges qui leur sont confiés. Ce n'est pas toujours le cas. Mais même dans de telles hypothèses, la Convention modernisée prévoit qu'à tout le moins, toute personne doit pouvoir

« bénéficier, quelle que soit sa résidence, de l'assistance d'une autorité de contrôle au sens de l'article 12*bis*, pour l'exercice des droits prévus par la présente Convention ».[66]

Ce droit à l'assistance des autorités de contrôle sera particulièrement précieux dans les situations transfrontières, dans lesquelles la personne concernée réside dans un pays tandis que le responsable du traitement des données est établi dans un autre pays.

Cette hypothèse dans laquelle les personnes concernées relevant d'un autre Etat peuvent être efficacement aidées avait d'ailleurs été déjà envisagée en 1981 mais n'était pas formulée sous forme de droit et ne faisait pas encore intervenir les autorités de contrôle car celles-ci n'avaient pas leur place dans la Convention. L'article 14, § 1er de l'actuelle version de la Convention dispose ainsi que « Chaque Partie prête assistance à toute personne ayant sa résidence à l'étranger pour l'exercice des droits prévus par son droit interne donnant effet aux principes énoncés à l'article 8 de la présente Convention. » La formule proposée sous forme de droit et ciblant précisément l'aide des autorités de contrôle est assurément plus percutante.

I. Devoirs des acteurs

Grande nouveauté dans la Convention modernisée, des devoirs devraient désormais peser sur les acteurs principaux des traitements de données. Une obligation de prendre des mesures de sécurité était certes déjà prévue dans la version de 1981 de la Convention mais rien n'indiquait sur qui pesait cette

[65] Rapport explicatif du Protocole additionnel à la Convention, point 13.
[66] Art. 8, g), du projet de texte.

obligation. Il a été décidé d'introduire des devoirs en matière de transparence et de sécurité élargie auxquels devraient venir s'ajouter encore des devoirs spécifiques complémentaires. Le texte clarifie cette fois sur qui pèsent ces nouvelles obligations et l'on verra que le responsable n'est pas le seul visé par les dispositions. L'éventuel sous-traitant se voit aussi réserver des obligations. Les concepteurs de produits et services d'information devront également tenir compte d'une nouvelle obligation envisagée dans le texte en projet.

I. Transparence

Un système de protection des données qui se veut crédible aujourd'hui ne peut plus s'accommoder de garanties qui reposent essentiellement sur la seule initiative de la personne concernée. Il est impératif, vu l'environnement particulièrement opaque des systèmes d'information actuels, de mettre à charge des responsables de traitement des obligations de transparence active. La personne concernée ne peut s'intéresser à et s'informer sur un traitement dont elle ne soupçonne pas l'existence. Combien de personnes concernées « standard » songeront que les mots introduits dans un moteur de recherche sont enregistrés pendant des mois et reliés à un pointeur identifiant ? Ou que des caméras les filment alors qu'elles sont miniaturisées et, vu leur puissance, posées à bonne distance ? Ou que leur entreprise conserve toutes les traces d'utilisation de clés/cartes magnétiques pour contrôler leurs déplacements ? Ou que le portique qu'elles franchissent lit la puce RFID qui se trouve dans leur passeport ? Les exemples de telles situations où les personnes concernées ne se doutent pas, tant qu'on ne les en a pas informées, que leurs données sont traitées, sont malheureusement multipliables à l'envi aujourd'hui.

Il a donc été rapidement décidé lors du travail de modernisation de la Convention d'introduire de façon expresse une *obligation d'information* des personnes sur lesquelles on traite des données, à mettre à charge des personnes qui effectuent le traitement. Cette obligation prend la forme suivante :

« Chaque Partie prévoit que le responsable du traitement garantit la transparence du traitement de données en informant les personnes concernées de son identité et sa résidence habituelle ou lieu d'établissement, des finalités des traitements qu'il effectue sur les données traitées, des destinataires ou catégories de destinataires des données, et des moyens d'exercer les droits énoncés à l'article 8, ainsi que de toute autre information nécessaire pour garantir un traitement loyal et licite des données. »[67]

[67] Art. 7*bis*, § 1 du projet de texte.

Une série de renseignements doivent donc être communiqués spontanément aux personnes sur qui on traite des données : nom et adresse du responsable du traitement, finalités du traitement, destinataires des données et information concrète sur les droits pouvant être exercés. Parmi les « autre[s] information[s] nécessaire[s] pour garantir un traitement loyal et licite des données », figure notamment l'information sur les pays tiers vers lesquels les données seront communiquées dans le cas où elles sont effectivement destinées à partir vers l'étranger.

Etant donné que la Convention doit présenter un texte rédigé à un niveau de généralité correspondant à un traité international, il ne convient pas d'aller trop loin dans le détail en indiquant par exemple à quel moment l'information doit être fournie par le responsable du traitement.

Il est prévu d'autoriser deux *exceptions* particulières à ce devoir d'information, en plus des possibilités d'exceptions ouvertes à l'article 9 de la Convention.[68] Ces deux exceptions particulières, tout à fait légitimes, n'entrent en effet pas dans les justifications d'exception admises à l'article 9, justifications fondées sur la sauvegarde d'intérêts publics ou privés prépondérants. L'une des exceptions tient compte de contraintes purement matérielles : le responsable du traitement n'est pas tenu de fournir les informations lorsque cela lui est impossible ou implique des efforts disproportionnés. La deuxième exception est accordée pour les traitements prévus par la loi. L'adage « nul n'est censé ignorer la loi » permet de considérer que les citoyens sont déjà informés mais cela n'est valable qu'à la condition que la loi en question soit suffisamment précise et apporte les renseignements nécessaires pour assurer une information loyale des personnes concernées.

II. Sécurité

1. Mesures de sécurité

Ainsi qu'on l'a dit ci-dessus, un devoir d'adopter des mesures de sécurité existe déjà dans le texte initial de la Convention. Il est repris dans la proposition de texte révisé mais, au passage, la *responsabilité de la sécurité* est éclaircie : elle revient au responsable du traitement ainsi qu'au sous-traitant dans les cas où il est recouru aux services d'un sous-traitant. L'article 7 dédié à la « sécurité des données » dans sa forme nouvelle se lit comme suit :

« Chaque Partie prévoit que le responsable du traitement, ainsi que le cas échéant le sous-traitant, prend des mesures de sécurité appropriées contre la modification, la perte ou la destruction accidentelles ou non autorisées de données à caractère personnel, ainsi que contre l'accès à ces données, leur diffusion ou leur divulgation non autorisés. »

[68] Art. 7*bis*, § 2 du projet de texte.

C'est aux Etats qu'il reviendra de donner une forme plus précise à l'exigence de sécurité. On signale que la jurisprudence a déjà apporté des éclaircissements intéressants sur la portée de cette exigence. Il en découle que les mesures de sécurité doivent non seulement empêcher les accès non autorisés mais également permettre aux personnes concernées de contrôler les accès aux données qui ont eu lieu. Seul cet *accès aux données sur les personnes ayant accédé aux données* permet en effet à la personne concernée de vérifier l'effectivité des mesures de sécurité et lui permet d'exercer son contrôle ou sa maîtrise sur ses propres informations. C'est en ce sens qu'a jugé la Cour européenne des droits de l'Homme dans l'affaire *I c. Finlande*, condamnant cet Etat pour avoir laissé un hôpital public mettre en place un système de sécurité des données qui ne conserve en mémoire que les traces des cinq derniers accès aux données et qui, de surcroît efface toute trace d'accès une fois les données versées aux archives.[69]

La Cour de Justice de l'Union européenne a, pour sa part, affirmé dans son arrêt *Rijkeboer*[70] que la protection des données implique que la personne concernée puisse s'assurer que ses données à caractère personnel sont adressées à des destinataires autorisés. Afin de pouvoir effectuer les vérifications nécessaires, la personne concernée doit disposer d'un droit d'accès à l'information sur les destinataires ou les catégories de destinataires des données ainsi qu'au contenu de l'information communiquée non seulement pour le présent, mais aussi pour le passé. Cela implique *l'obligation de conservation pendant une certaine durée des renseignements relatifs aux personnes destinataires* des données ainsi qu'aux données précisément consultées ou transmises.

Signalons encore que même si le texte n'est pas explicite à ce propos, se contentant de mentionner des mesures de sécurité « appropriées », le Rapport explicatif spécifie qu'il faut entendre par là que les mesures de sécurité doivent être adaptées aux fonctions spécifiques du traitement de données et proportionnées aux risques encourus. *L'exigence de sécurité est* donc *modélisable* en fonction de la nature des données, des circonstances qui entourent leur traitement et des risques que celui-ci fait courir aux personnes concernées. La Cour européenne des droits de l'Homme a, dans le cours de son

[69] Cour eur. D.H., *I. v. Finlande*, 17 July 2008, appl. n° 20511/03, § 41.

[70] C.J.U.E., 7 mai 2009, (*Rijkeboer*), aff. C-553/07. Voy. sur ce point *Cécile de Terwangne*, L'étendue dans le temps du droit d'accès aux informations sur les destinataires de données à caractère personnel, note sous C.J.U.E, 7 mai 2009, *R.D.T.I.*, 2011, n°43, pp. 65-81

argumentation dans l'arrêt *I c. Finlande*,[71] mis en exergue que la confidentialité de certaines données (par exemple les données médicales) présentant une importance plus grande pour les individus concernés imposait dans ces cas des mesures de sécurité plus strictes. Dans la même ligne, la directive 2002/58 sur la protection de la vie privée dans les communications électroniques[72] dispose, dans son article 4 consacré à la sécurité du traitement : « [...] Compte tenu des possibilités techniques les plus récentes et du coût de leur mise en œuvre, ces mesures garantissent un degré de sécurité adapté au risque existant. » L'APEC *Privacy Framework*[73] ainsi que la Résolution de Madrid[74] présentent tous deux la même modulation des exigences de sécurité.

2. *Violation des données*

Un paragraphe supplémentaire va vraisemblablement être ajouté à l'article 7 sur la sécurité des données. Il s'agit de l'insertion dans la Convention d'une règle portant sur les « violations des données ». Cette règle s'énoncera de la sorte :

> « 2 Chaque Partie prévoit que le responsable du traitement est tenu de notifier immédiatement à tout le moins aux autorités de contrôle au sens de l'article 12*bis* de la présente Convention les violations des données susceptibles de porter gravement atteinte aux droits et libertés fondamentales des personnes concernées. »[75]

Venue des Etats-Unis où une grande majorité des Etats ont adopté une législation à ce propos, cette préoccupation relative aux *privacy breaches* a reçu un écho dans la législation communautaire européenne.[76] Telle qu'elle

[71] Cour eur. D.H., *I. v. Finlande*, 17 juillet 2008, appl. n° 20511/03.

[72] Directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive « vie privée et communications électroniques »).

[73] Son Principe VII *Security Safeguards* stipule : « 22. Personal information controllers should protect personal information that they hold with appropriate safeguards [...]. Such safeguards should be proportional to the likelihood and severity of the harm threatened the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment. ».

[74] Article 20, § 1, *in fine:* « These measures depend on the existing risk, the possible consequences to data subjects, the sensitive nature of the personal data, the state of the art, the context in which the processing is carried out, and where appropriate the obligations contained in the applicable national legislation. »

[75] Art. 7, § 2, du projet de texte.

[76] Ainsi, la directive 2002/58 sur la protection de la vie privée dans les communications électroniques a été amendée par la directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 en vue notamment d'y introduire une disposition spécifique aux « violation de données à caractère personnel ».

est énoncée dans le projet de texte révisé de la Convention, la règle demande que tout responsable du traitement informe des problèmes de sécurité qui sont survenus.

Il s'agit ainsi d'aviser à tout le moins aux autorités de contrôle (éventuellement aussi les personnes concernées si l'Etat Partie le prévoit dans sa législation transposant la Convention) lorsqu'un tiers non autorisé, un pirate par exemple, a accédé à des données à caractère personnel en s'introduisant illégalement dans un serveur. Entrent également dans le champ de cette obligation des situations dans lesquelles les données à caractère personnel ont été perdues (par exemple, sur des CD-Rom, des clés USB ou d'autres appareils portatifs), ou communiquées par inadvertance ou malveillance par un utilisateur autorisé, en violation du principe de finalité ou de son devoir de confidentialité (par exemple, un fichier de données bancaires transmis aux autorités fiscales d'un pays tiers par un employé licencié, à titre de vengeance ; la publication accidentelle sur un site internet de la liste des personnes affiliées à un parti politique ; l'envoi par une société pharmaceutique d'un mail d'alerte à propos d'un médicament laissant apparaître le nom et les coordonnées de toutes les personnes consommant ce médicament, ...).

Les avantages liés à une telle obligation d'informer sur les violations de la sécurité et compromissions des données sont importants sur le plan de la protection des données : « Les notifications des violations de la sécurité peuvent aider les personnes à prendre les mesures qui s'imposent pour réduire les dommages susceptibles de résulter d'une telle compromission. En outre, l'obligation de notifier les violations de la sécurité incitera les sociétés à améliorer la sécurité des données et les rendra davantage comptables des données à caractère personnel dont elles sont responsables. »[77]

On remarquera que le texte proposé évoque un *seuil de gravité du préjudice susceptible de découler de la violation des données* pour que naisse l'obligation de notification de cette violation. Il ne s'agit pas de noyer les autorités de contrôle voire les personnes concernées avec tant de messages insignifiants que la fonction d'alerte serait émoussée et que l'on n'atteindrait pas l'objectif voulu.

On notera en outre que l'obligation pèse ici sur n'importe quel responsable du traitement. Elle n'est pas cantonnée à une catégorie de responsables

[77] Deuxième avis du contrôleur européen de la protection des données relatif au réexamen de la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive «vie privée et communications électroniques»), *J.O.U.E.*, 6 juin 2009, C 128/28, par. 10.

liée à une matière particulière.[78] Cette obligation s'adressera donc aux banques en ligne, aux entreprises qui ont développé des activités sur le réseau, aux prestataires de services de soins de santé en ligne, etc.

III. Autres devoirs complémentaires

Une disposition nouvelle, l'article 8*bis*, est introduite dans le projet de Convention modernisée pour ajouter aux obligations de transparence et de sécurité des obligations complémentaires.

1. Accountability principle

Tout d'abord, il s'agit pour le responsable du traitement, ou le cas échéant le sous-traitant, de

> « prendre à toutes les étapes du traitement toutes les mesures appropriées pour mettre en œuvre les dispositions donnant effet aux principes et obligations de la présente Convention et mettre en place des mécanismes internes pour vérifier et démontrer aux personnes concernées et aux autorités de contrôle prévues à l'article 12*bis* de la présente convention la conformité des traitements de données dont il est responsable au regard du droit applicable. »[79]

C'est là une formulation succincte de ce qu'on a appelé le *accountability principle*.[80] Il impose de mettre en place des mécanismes internes permettant de démontrer la conformité des traitements avec les dispositions applicables.

La Résolution de Madrid contient une disposition allant dans le même sens. Son article 11 intitulé « *Accountability principle* » prévoit pour la personne responsable, à côté de l'obligation de prendre toutes les mesures nécessaires pour se conformer aux règles de protection, l'obligation de mettre

[78] Voy. la critique qui avait été émise au sein de l'Union européenne face au fait que l'obligation d'informer les personnes des violations de sécurité soit limitée aux seuls fournisseurs de service de communications électroniques accessibles au public (soit les sociétés de télécommunications et les fournisseurs d'accès internet) (Deuxième avis du contrôleur européen de la protection des données relatif au réexamen de la directive 2002/58/CE, précité, par. 22 et s.). Pour le Groupe de l'article 29, « élargir la portée de l'obligation aux prestataires de services de la société de l'information en général augmenterait leur responsabilité et contribuerait à sensibiliser le public. Cela permettrait incontestablement de réduire les risques en matière de sécurité. » (Groupe de l'article 29, WP 150, avis 2/2008 sur la révision de la directive 2002/58/CE concernant la protection de la vie privée dans le secteur des communications électroniques (« directive vie privée et communications électroniques »), 15 mai 2008).

[79] Art. 8*bis*, § 1er, du projet de texte.

[80] Voy. Groupe de l'article 29, Avis n° 3/2010 sur le principe de la responsabilité, WP 173 du 13 juillet 2010, point 3.

en place les mécanismes internes permettant de démontrer qu'il s'est précisément conformé à ces règles.

2. Analyse de risques et obligation de minimisation des risques

Pèse en outre sur les seuls responsables de traitement cette fois, l'obligation de procéder à une analyse de risques et de concevoir les traitements de manière à minimiser ces risques :

> « Chaque Partie prévoit que le responsable du traitement, est tenu de procéder à une analyse de l'impact potentiel du traitement de données envisagé sur les droits et libertés fondamentales des personnes concernées et de concevoir les traitements de données de manière à prévenir ou pour le moins à minimiser les risques d'atteinte à ces droits et libertés fondamentales. »[81]

On peut voir dans ces évaluations des incidences que le produit ou service en question risque d'avoir la manifestation de la mise en balance des droits et intérêts qui devrait précéder le lancement de tout traitement de données (cf. *supra* le point F.I.). Cette obligation de mettre par écrit la mise en balance garantit que l'on a effectivement procédé à une prise en considération de tous les intérêts en jeu et permettrait de contester plus facilement, le cas échéant, le résultat de cette mise en balance.

Les Etats Parties seront libres de moduler ces exigences en fonction de la taille de l'entreprise concernée (responsable du traitement ou sous-traitant) et en fonction du volume de données traitées et des risques pour les intérêts, droits et libertés fondamentales des personnes concernées. Cette possibilité d'aménagement ou de dérogation doit permettre d'éviter de mettre en place des obligations matérielles trop lourdes aux yeux de certains types de responsables de traitement.

3. Prise en compte du respect de la vie privée dès la conception (Privacy by Design)

Le principe de « prise en compte de la vie privée dès la conception » (*Privacy by Design*) apparaît de plus en plus comme une exigence incontournable aujourd'hui pour réaliser efficacement la protection de la vie privée et des données.[82] Cette exigence d'intégration de la préoccupation de protection de

[81] Art. 8*bis*, § 2, du projet de texte.

[82] La proposition de règlement général de l'UE sur la protection des données nuance opportunément entre principes de protection des données dès la conception et de protection des données par défaut (voy. l'article 32 de la Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du

la vie privée au sein même des systèmes, produits et services créés et dès les premiers stades de leur conception permet d'offrir une protection effective à bien moindre frais que lorsqu'il faut intégrer les préoccupations de protection de la vie privée et des données par la suite, une fois le produit conçu et opérationnel.

L'article 8*bis*, § 3 tel que proposé stipule dans cet esprit :

« Chaque Partie prévoit que les produits et services destinés au traitement de données doivent prendre en compte les implications du droit à la protection des données à caractère personnel dès leur conception et faciliter la conformité des traitements de données au regard du droit applicable. »

J. Flux transfrontières de données

La question des flux transfrontières de données fait pour l'heure l'objet de deux dispositions différentes, insérées dans deux instruments juridiques différents. L'article 12 actuel de la Convention porte sur les flux transfrontières de données intra-Parties, tandis que l'article 2 du Protocole additionnel de 2001 traite des flux à destination de pays tiers à la Convention.

Il est envisagé de rassembler les approches et de traiter l'ensemble des flux transfrontières dans une seule disposition.

On signalera d'emblée que cette disposition fait encore à l'heure actuelle l'objet de nombreuses discussions parmi les personnes responsables de la modernisation de la Convention, conduisant à modifier régulièrement de façon conséquente le texte proposé. Il ne s'indique donc pas de présenter de façon approfondie la dernière version de l'article 12 renouvelé de la Convention car trop d'incertitudes pèsent sur le sort de cette version.[83]

traitement des données à caractère personnel et à la libre circulation de ces données (Règlement général sur la protection des données), COM (2012) 11/4, 25 janvier 2012).

[83] Dans sa version de fin septembre, l'article 12 en projet stipule :

1. Les dispositions suivantes s'appliquent à la communication ou à la mise à disposition de données à un destinataire qui ne relève pas de la juridiction de la Partie dont émanent ces données.
2. Une Partie ne peut, aux seules fins de la protection des données, interdire ou soumettre à une autorisation spéciale la communication ou la mise à disposition des données à un destinataire relevant de la juridiction d'une autre Partie à la Convention, à moins que la Partie dont émane les données ne soit régie par des règles régionales harmonisées de protection et que la communication ou la mise à disposition des données ne puisse être encadrée par des mesures visées au paragraphe 4.b.
3. Lorsque le destinataire relève de la juridiction d'un Etat ou d'une organisation internationale qui n'est pas Partie à la Convention, la communication ou la mise à disposition des données n'est possible que si un niveau approprié de protection des données à caractère personnel est assuré.

On relèvera néanmoins que si la notion de flux transfrontières est maintenue au niveau de l'intitulé de la disposition, cette notion est illustrée au sein même de l'article par l'expression « *la communication ou la mise à disposition de données* ». Cela permet de faire entrer dans la notion les situations du *cloud* dans lesquelles, sans qu'il y ait véritablement de mouvement de données, ces dernières sont rendues accessibles à des personnes se situant au-delà des frontières.

C'est donc « à la communication ou à la mise à disposition de données à un destinataire qui ne relève pas de la juridiction de la Partie dont émanent ces données »[84] que s'appliquent les dispositions figurant sous le titre de flux transfrontières de données.

Une des difficultés majeures qui expliquent que la disposition soit encore âprement discutée consiste dans le fait que la solution qui sera choisie pour figurer dans la Convention modernisée doit être parfaitement compatible avec le régime des flux transfrontières instauré par l'Union européenne. Cela est indispensable pour les Etats membres de l'UE, sous peine de les voir tiraillés entre des obligations contradictoires.

Les grands axes de protection appelés à figurer dans la disposition peuvent tout de même être exposés. L'idée est de proclamer tout d'abord que la *liberté des flux transfrontières entre Parties à la Convention est garantie.*

4. Un niveau de protection des données approprié peut être assuré par :
a) Les règles de droit de cet Etat ou de cette organisation internationale, notamment les traités ou accord internationaux applicables, ou
b) des mesures juridiques standardisées agréées ou ad hoc ; ces dernières devant être contraignantes, susceptibles de recours effectifs et mises en œuvre par la personne qui communique ou rend accessibles les données à caractère personnel et par le destinataire.
5. Nonobstant les modalités prévues aux paragraphes 2, 3 et 4, chaque Partie peut prévoir que la communication ou la mise à disposition des données peut avoir lieu, si dans un cas particulier :
a) la personne concernée a donné son consentement spécifique, libre et [explicite/non-équivoque], après avoir été informée des risques dus à l'absence de garanties appropriées ; ou
b) des intérêts spécifiques de la personne concernée le nécessitent ; ou
c) des intérêts légitimes protégés par la loi et répondant aux critères de l'article 9 prévalent.
6. Chaque Partie prévoit que l'autorité de contrôle compétente au sens de l'article 12*bis* de la Convention soit informée des modalités encadrant les flux de données, notamment des mesures ad hoc prises au sens de l'article 12, paragraphe 4.b. Elle prévoit également que l'autorité de contrôle puisse exiger de la personne qui communique ou rend accessibles les données ou du destinataire de démontrer la qualité et l'effectivité des mesures prises, ou que celle-ci puisse interdire, suspendre ou soumettre à condition la communication des données ou leur mise à disposition au sens des paragraphes 4, lettre b ou 5 [lettres a et b].

[84] Art. 12, § 1, du projet de texte.

Toutefois cette liberté n'est pas systématique, et c'est ici que l'on tente de gérer la contrainte de la coordination entre les deux sphères juridiques européennes. Un Etat Partie pourrait, aux seules fins de la protection des données, interdire ou soumettre à une autorisation spéciale la communication ou la mise à disposition des données à un destinataire relevant de la juridiction d'une autre Partie à la Convention, dans l'hypothèse où il serait régi par des règles régionales harmonisées. Il s'agit donc d'être soumis à la contrainte du respect de règles collectives et non édictées individuellement et souverainement par l'Etat Partie.

Pour les flux « vers » un destinataire relevant de la juridiction d'Etats non-Parties à la Convention, la règle serait qu'ils ne seront *autorisés que si une protection appropriée* est offerte aux données transmises. On se dirige sans doute vers l'usage d'un vocabulaire différent de celui repris au sein de l'Union européenne, afin de ne pas conduire à la situation pénible pour les acteurs de terrains où un mot (la protection adéquate, en l'occurrence) aurait deux significations différentes selon qu'il est utilisé dans le contexte de l'Union européenne ou dans celui du Conseil de l'Europe.

La protection appropriée pourrait découler:

a) des règles de droit de l'Etat du destinataire ou de l'organisation internationale, notamment des traités ou accord internationaux applicables, ou

b) de mesures juridiques standardisées agréées ou *ad hoc*.

Dans le cas de mesures *ad hoc*, pour être admises elles doivent être contraignantes, susceptibles de recours effectifs et mises en œuvre par la personne qui communique ou rend accessibles les données à caractère personnel ainsi que par le destinataire.

Il sera vraisemblablement prévu qu'il faut *informer* (et non demander un feu vert à) *l'autorité de contrôle* des mesures *ad hoc* prises pour assurer un niveau de protection des données approprié. Si l'autorité n'a pas à donner son autorisation, elle devrait par contre disposer du pouvoir de vérifier sur le terrain la qualité et l'effectivité des mesures prises.

Enfin, des *exceptions* devraient être prévues pour permettre de transmettre des données sans protection appropriée.

K. Autorités de contrôle

En 1981 nul n'a songé à évoquer des autorités de contrôle spécifiques dans la Convention 108. Vingt ans plus tard, la volonté s'est fait jour de renforcer la protection effective de l'individu par le biais de la création d'une ou plusieurs autorités de contrôle qui contribuent à la protection des droits et libertés de l'individu à l'égard du traitement des données. L'expérience acquise

durant ces vingt années a en effet démontré que lorsqu'elles sont dotées de compétences effectives et qu'elles jouissent d'une réelle indépendance dans l'exercice de leurs fonctions, de telles autorités sont devenues partie intégrante du système de contrôle de la protection des données dans une société démocratique.

Un nouveau chapitre consacré aux autorités de contrôle transposera dans la Convention les dispositions contenues à ce propos jusqu'à présent à l'article 2 du protocole additionnel de 2001. L'article 12*bis* de la Convention révisée devrait reprendre assez fidèlement le texte du protocole si ce n'est sur deux points. La disposition vise premièrement à renforcer l'indépendance de ces autorités de contrôle, notamment en précisant que ces autorités ne peuvent solliciter ni accepter d'instructions de quiconque. Le texte vise deuxièmement à renforcer les pouvoirs des autorités. Il précise à cet effet que

> « ces autorités :
>
> a. disposent de pouvoirs d'investigation et d'intervention ;
>
> b. sont compétentes en matière de flux transfrontières de données et peuvent marquer leur agrément de clauses juridiques standardisées ;
>
> c. peuvent prononcer les décisions nécessaires au respect des mesures du droit interne donnant effet aux dispositions de la présente Convention et notamment sanctionner les infractions administratives ;
>
> d. disposent du pouvoir d'ester en justice ou de porter à la connaissance de l'autorité judiciaire compétente des violations aux dispositions du droit interne donnant effet aux dispositions de la présente Convention ;
>
> e. sont chargées de sensibiliser et d'éduquer à la protection des données. »[85]

On relèvera que le renforcement le plus remarquable se situe à l'alinéa c) évoquant un pouvoir de décision et de sanction autonome des autorités de contrôle. Par ailleurs, les autorités se voient confier une mission pédagogique en matière de protection des données, ce qui est assurément très pertinent si l'on prend en compte le contexte actuel dans lequel s'effectuent les traitements des données. La mission de sensibilisation et d'éducation devrait s'exercer à l'égard du public qu'il convient d'éveiller aux risques. Mais il s'agirait aussi de sensibiliser les responsables de traitements sur les règles à respecter pour garantir un équilibre entre tous les intérêts en présence.

[85] Art. 12*bis*, § 2, du projet de texte.

Bibliographie

Burkert, Herbert : Le jugement du tribunal constitutionnel fédéral allemand sur le recensement démographique, Droit de l'Informatique et des Télécoms, 1985, 8 ss.

de Terwangne, Cécile : « L'étendue dans le temps du droit d'accès aux informations sur les destinataires de données à caractère personnel », note sous C.J.U.E, 7 mai 2009, R.D.T.I., 2011, n°43, 65-81.

de Terwangne, Cécile : Le rapport de la vie privée à l'information, in : Droit des technologies de l'information. Regards prospectifs (sous la direction d'E. Montero), coll. Cahiers du CRID, n° 16, Bruxelles, Bruylant, 1999, 144 ss.

de Terwangne, Cécile/Moiny, Jean-Philippe : Les lacunes de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108) face aux développements technologiques, Rapport pour le Conseil de l'Europe, Strasbourg Novembre 2010, 60 p., disponible à l'adresse <http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports_and_studies_fr.asp>.

de Terwangne, Cécile/Moiny, Jean-Philippe : Rapport sur la consultation relative à la modernisation de la Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Conseil de l'Europe, Strasbourg juin 2011, disponible à <http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD-BUR_2011_10_fr.pdf>.

Gautrais, Philippe : Guide relatif à la gestion des documents technologiques, Fondation du Barreau du Québec, 2005, 8, disponible à l'adresse <http://lccjti.ca/definition/neutralite-technologique/>.

Korff, D. : Data protection laws in the EU : The difficulties in meeting the challenges posed by global social and technical developments, EC Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments, WP 2, 20 January 2010.

Leonard, Thierry/Poullet, Yves : Les libertés comme fondement de la protection des données nominatives, in : F. Rigaux, La vie privée : une liberté parmi les autres ?, Travaux de la faculté de Droit de Namur, n° 17, Bruxelles, Larcier, 1992, 231 ss.

Poullet, Yves/Rouvroy, Antoinette : Le droit à l'autodétermination informationnelle et la valeur du développement personnel : une réévaluation de l'importance du droit à la protection de la vie privée pour la démocratie, in : Karim Benyekhlef/Pierre Trudel, Etat de droit et virtualité, Montréal 2009, 157 ss.

Poullet, Yves/Dinant, Jean-Marc/de Terwangne, Cécile/Perez-Asinari, Maria-Veronica : L'autodétermination informationnelle à l'ère de l'Internet, Rapport pour le Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD), Conseil de l'Europe, Strasbourg, 18 novembre 2004.

Simitis, Spiros : Les données sensibles revisitées (1999), Examen des réponses au questionnaire du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE 108), Strasbourg, 24-26 novembre 1999.